SAG-18-0648 MJM

AFFIVADIT IN SUPPORT OF APPLICATION FOR SEARCH & SEIZURE WARRANTS

I, Special Agent Bradford J. Lynch, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am employed as a Special Agent with the Federal Bureau of Investigation (FBI) and have worked in that capacity since January 1998. I am an "investigative or law enforcement officer" of the United States, within the meaning of Section 2510 (7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Sections 1028A, 1029, 1343, and 1344 of Title 18 of the United States Code, and related offenses.

2. I have attended the training course for Special Agents at Quantico, Virginia, and have training in bank robbery, violent crime, counterintelligence, counterterrorism, narcotics and white collar crime investigations. I am currently assigned to the Baltimore Division, where I have investigated bank robbery and fugitive matters, foreign counterintelligence, and counterterrorism. I have been assigned for the past eight years to work white collar crime matters which include mail fraud, wire fraud, bank fraud, mortgage fraud and healthcare fraud. I have attended additional training classes on mortgage fraud, money laundering, and healthcare fraud. I have drafted several arrest warrants and search warrants, having been trained in the requirements for probable cause, and have participated in several searches, arrests, and seizure warrants involving a variety of federal offenses.

3. This Affidavit is being submitted in support of an application for a search warrant for various digital media of Andre Elroy Williams ("**WILLIAMS**"). I respectfully submit that probable cause exists to believe that the electronic devices described in Attachment A contain

evidence, and are themselves instrumentalities of criminal conduct committed by **WILLIAMS** and others identified and unidentified.

THE TARGET DEVICES

4. The Target Devices to be examined are described herein and further described in Attachment A. The devices were recovered on April 12, 2017, when they were seized subsequent to a Maryland state search warrant signed by the Honorable N.M. Purpura. The search was executed at 1611 W. Mulberry Street, Baltimore, Maryland. The Target Devices are listed below with evidence numbers and a brief description:

a. 1B-1 Black Dell Laptop Model Inspiron 15 SN# 2GPP8B2
b. 1B-2 Black Dell Laptop Model Inspiron 15 SN# C3BQC12
c. 1B-3 Samsung Tablet Model SM-T810 SN # R52H40QDMKD
d. 1B-4 SILVER IPHONE S, MODEL A1634, IC: 579C-E2944
e. 1B-5 SILVER IPOD, MODEL A1574, SN CCQQ84JBGGNL
f. 1B-6 GOLD IPHONE MODEL A1522, IMEI: 355878062124284 WITH CRACKED SCREEN
g. 1B-7 BLACK ALCALTEL FLIP PHONE MODEL ONETOUCH, S/N 014570000467098
h. 1B-8 BLACK KYOCERA QUALCOMM, MODEL C674ON, IMEI: 014249008202571
i. 1B-9 BLACK SAMSUNG GALAXY J36V, SM-J320V, IMEI: 355076081125396
j. 1B10 SILVER HP LAPTOP PAVILION, MODEL 15-AU158NR, SN #5CD7051D57 or 5CD705ID57

5. The applied-for warrant would authorize the forensic examination of the Target Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

6. Based on my investigation to date, your Affiant respectfully submits there is probable cause to believe that there is evidence located on the Target Devices of the following

illegal activity: bank fraud, in violation of Title 18, United States Code, Section 1344; (2) access device fraud, in violation of Title 18, United States Code, Section 1029; and (3) aiding and abetting of these crimes, in violation of Title 18, United States Code, Section 2, among other federal crimes.

7. The facts set forth in this Affidavit are based upon my personal knowledge, knowledge obtained during my participation in this investigation, knowledge obtained from other investigators, a review by myself and other investigators of documents related to this investigation, communications with others, and information gained through my training and experience. This Affidavit is submitted for the limited purpose of establishing probable cause in the support of these applications for search warrants, and thus, it does not contain every fact known by myself or the Government.

PROBABLE CAUSE

8. Andre Elroy Williams ("**WILLIAMS**") was convicted of Possession of Stolen Mail in violation of 18 U.S.C. § 1708 and Use of Unauthorized Access Devices in violation of 18 U.S.C. § 1029 in the U.S. District Court for the District of Maryland in 2004. On July 22, 2004, **WILLIAMS** was sentenced to a prison term of 45 months to be followed by three years of supervised release. Based on violations of conditions of supervised release, supervised release was revoked in 2008, and **WILLIAMS** was sentenced to an additional 10 months in prison.

9. On or about March 15, 2017, E.S. contacted the Baltimore County Police Department to report that two counterfeit checks had been cashed against her bank account without her authorization. E.S. reported that, after checking the balance of an account she held at M&T Bank and learning that there were no funds in the account, she and an M&T Bank

representative learned that two checks were cashed against her account that she did not write or authorize. After reviewing copies of the checks, E.S. discovered that the checks were counterfeit. Examination of each check revealed that the issuing bank was listed as Bank of America and the accountholder was listed as "United States Fugitive Apprehension Unit Inc." located at 302 N. Gilmore (*sic*) Street, Baltimore, Md. 21223. However, the M&T Bank routing number was listed on each check with E.S.'s checking account number.

10. Each check indicated that it was written on March 2, 2017. One check (#1510) was written to Micro Center in the amount of $529.99, and the other check (#1511) was written to Microsoft in the amount of $2,012.94. Further investigation confirmed that, on March 2, 2017, check #1510 was uttered at a Micro Center retail location in the Perring Plaza Shopping Center in Parkville, Maryland, and check #1511 was uttered at a Microsoft Store retail location at Towson Town Center in Towson, Maryland. A receipt from the Micro Center location reflected that check #1510 was used to purchase a Pavilion laptop computer for a total cost of $529.99. The customer name was listed as "U.S. Fugitive Apprehension Unit, Andre Williams." A receipt from the Microsoft Store location reflected that a customer named "Andre Williams" with an email address of **usfau81@outlook.com** used check #1511 to purchase a Microsoft laptop computer for a total cost of $2,012.94 on March 2, 2017, at approximately 7:24 p.m. **WILLIAMS** was captured in surveillance images from Perring Plaza Shopping Center and Towson Town Center on March 2, 2017.

11. Articles of Incorporation for United States Fugitive Apprehension Unit, Inc. lists **WILLIAMS** as the incorporator and resident agent, and lists 1611 W. Mulberry Street, Baltimore, Maryland as the street address for the principal office and 302 N. Gilmor Street,

Baltimore, Maryland as **WILLIAMS**'s address. Based on **WILLIAMS**'s status as incorporator and resident agent of United States Fugitive Apprehension Unit, Inc., I believe that the "usfau" in the aforementioned email address stands for "United States Fugitive Apprehension Unit."

12. On April 12, 2017, Baltimore County Police Department arrested **WILLIAMS** at 1611 W. Mulberry Street, Baltimore, Maryland. A Maryland state search warrant was subsequently executed at the same location. During execution of the search warrant, officers recovered the Target Devices, more than 70 checks, more than 30 debit cards in different names, at least six social security cards, approximately 19 driver's licenses for individuals with no apparent connection to the Mulberry Street location, and several notes listing personal identifying information for various individuals. The dates on checks recovered from the Mulberry Street location ranged from approximately June 2010 to April 2017, and the checks ranged in value from a blank check to over $8,000. Remitters listed on the checks included **WILLIAMS,** companies connected to **WILLIAMS** (i.e., U.S. Fugitive Apprehension Unit), and many other names and companies. Several checks appeared to be counterfeit, as indicated by routing numbers that do not match issuing banks listed on the checks, account numbers that do not belong to the remitters listed on the checks, and account numbers that were inactive or not legitimate. The following is a list of information listed on a sample of the checks recovered from the Mulberry Street location, each of which appears to bear the same signature of "Andre Williams":

	Remitter:	Pay to:	Date:	Phone:	Amount:
1.	Omni Investment	Best Buy	3/26/2016	410-831-0225	$1271.99
2.	Omni Investment	Apple	3/26/2016	410-831-0225	$1376.94

3.	Omni Investment	Best Buy	3/22/2016	410-831-0225	$399.52
4.	Andre Williams	Office Depot	1/30/2017	410-207-9394	$402.67
5.	Reliable Home Rep.	Home Depot	4/10/2017	410-220-2127	$271.38
6.	Williams&Wells	Staples	10/29/2016	410-831-0225	$1017.68

13. I have read police reports reflecting that persons calling a police agency from telephone number 410-831-0225 identified themselves as "Mr. Williams," "Agent Williams," or "Fugitive Agent Williams."

14. Verizon provides telephone service to 410-207-9394. Verizon records show the subscriber on this account is **WILLIAMS**, d/b/a Syndicate II Productions Management, with an alternative telephone number of 410-831-0225.

15. Your Affiant knows that to print counterfeit checks like those described above, one must have a computer and software in order to add or change routing numbers, account numbers, remitter information, bank information, and other information listed on a check.

16. Among the items recovered from the Mulberry Street location during the search on April 12, 2017, were an Anne Arundel Community College identification card belonging to B.D., a full checkbook and a driver's license belonging to K.O., and several items belonging to M.S., including a driver's license, AAA card, insurance card, bank card, and other identifying documents.

17. On February 28, 2016, B.D. reported to Anne Arundel County Police that, on that date, she put her wallet down while shopping for a cellular telephone at an AT&T kiosk in Arundel Mills Mall and walked away from the kiosk. She returned to the kiosk when she realized that she left her wallet but the wallet was missing. She advised Anne Arundel County

Police that her wallet contained her Anne Arundel Community College identification as well as other identification cards and credit, debit, and gift cards.

18. On February 8, 2018, I spoke with K.O., and she advised that on or about April 2, 2016, while she was working, she had left her purse in her car, which was parked at a location in Baltimore, Maryland. When she returned to her car, she found that her passenger side window was smashed and her purse was gone.

19. On February 9, 2018, I spoke with victim M.S., and he advised that, during a business trip to Baltimore in October 2016, he was assaulted and robbed of his wallet and personal belongings. According to a report by Baltimore Police Department, this assault and robbery occurred on or about October 23, 2016.

20. On February 7, 2018, **WILLIAMS** pleaded guilty to offenses relating to identity theft of E.S. and a scheme to steal laptop computers from Micro Center and the Microsoft Store on March 2, 2017.

21. Based on my training and experience, and the foregoing facts, there is probable cause to believe that **WILLIAMS** has engaged in bank fraud, in violation of 18 U.S.C. § 1344; aggravated identity theft, in violation of 18 U.S.C. § 1028A; and other criminal violations.

COMPUTERS AND OTHER ELECTRONIC STORAGE MEDIA

22. As described above and in Attachment B, this application seeks permission to search for data and records on the Target Devices, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media and the copying of electronically stored information, under Federal Rule of Criminal Procedure 41(e)(2)(B).

23. Based on my training and experience, and the foregoing facts, there is probable cause to believe that the Target Devices recovered from 1611 W. Mulberry Street, Baltimore, Maryland on April 12, 2017, contain evidence, fruits, and instrumentalities of criminal violations including bank fraud, in violation of 18 U.S.C. § 1344; fraud and related activity in connection with identification documents, in violation of 18 U.S.C. § 1028; and aggravated identity theft, in violation of 18 U.S.C. § 1028A; for at least the following reasons, based on my knowledge, training, and experience:

a. Participants in bank fraud and identity fraud schemes commonly use computers, cellular telephones, and other electronic devices to engage in voice calls, text messages, email, and social media contacts in order to conduct activities in furtherance of their crimes, including but not limited to the following: to communicate with co-conspirators, victims, and third-party banks and other businesses; to convey and/or receive personal identity and financial information, and other instrumentalities of their fraud schemes; and to conduct financial transactions.

b. Participants in bank fraud and identity fraud schemes maintain books, records and other documents that identify and contain the names, addresses and/or telephone numbers of other participants and of victims in locations including, but not limited to, computers, cellular telephones, and other electronic storage media.

c. Participants in bank fraud and identity fraud schemes maintain in electronic storage media (such as computers and cellular telephones) information necessary to execute their schemes as well as information obtained as a result of their crimes, including

personal identifying information and credit card and bank account information belonging to individual victims.

d. Creating counterfeit checks like those described in this affidavit requires use of a computer and software in order to add or change routing numbers, account numbers, remitter information, bank information, and other information listed on a check.

e. Electronic data files or remnants of such files can be recovered months or even years after they have been saved to a storage medium, deleted, or viewed via the Internet. Electronic files saved to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

f. Wholly apart from user-generated files, electronic storage media contain evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information.

g. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

h. Many cellular telephones have features that capture and store for long periods of time the telephone numbers of incoming and outgoing calls, contact lists that include names and telephone numbers, email, text messages, photographs, IP addresses, geographic locations, and voice recordings.

i. Users of cellular telephones commonly transfer information stored on cellular telephones to other electronic storage media (such as laptop computers) for backup storage.

j. Electronic storage devices, including computers and cellular telephones, commonly contain indicia of ownership and information identifying users of the devices. This "user attribution" evidence is analogous to "indicia of occupancy" commonly obtained while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

k. The Target Devices have remained in law enforcement custody since the date of their seizure from 1611 W. Mulberry Street, Baltimore, Maryland on April 12, 2017.

CONCLUSION

24. Based on the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the aforementioned crimes, described in Attachment B, is located on the electronic devices in Attachment A. I respectfully request that a search warrant be issued to examine the electronic devices listed in Attachment A for the items listed in

Attachment B.

Bradford J. Lynch, Jr.
Special Agent, FBI

Subscribed and sworn to before me this 7th day of March, 2018.

The Honorable Stephanie A. Gallagher
United States Magistrate Judge
District of Maryland

Attachment A

Locations to Be Searched

The following electronic devices, which were seized on April 12, 2017, and remain in the custody of FBI in Woodlawn, Maryland, are to be searched:

a. 1B-1 Black Dell Laptop Model Inspiron 15 SN# 2GPP8B2
b. 1B-2 Black Dell Laptop Model Inspiron 15 SN# C3BQC12
c. 1B-3 Samsung Tablet Model SM-T810 SN # R52H40QDMKD
d. 1B-4 SILVER IPHONE S, MODEL A1634, IC: 579C-E2944
e. 1B-5 SILVER IPOD, MODEL A1574, SN CCQQ84JBGGNL
f. 1B-6 GOLD IPHONE MODEL A1522, IMEI: 355878062124284 WITH CRACKED SCREEN
g. 1B-7 BLACK ALCALTEL FLIP PHONE MODEL ONETOUCH, S/N 014570000467098
h. 1B-8 BLACK KYOCERA QUALCOMM, MODEL C674ON, IMEI: 014249008202571
i. 1B-9 BLACK SAMSUNG GALAXY J36V, SM-J320V, IMEI: 355076081125396
j. 1B10 SILVER HP LAPTOP PAVILION, MODEL 15-AU158NR, SN #5CD7051D57 or 5CD705ID57

Attachment B

Items To Be Seized

I. Information to be Seized by Law Enforcement Personnel

The following items, which constitute fruits, evidence and instrumentalities of criminal violations of 18 U.S.C. § 1344 (bank fraud) and 18 U.S.C. § 1028A (aggravated identity theft) may be seized upon inspection of the locations listed in **Attachment A**:

1. Any and all books, records, and documents including but not limited to appointment books, diaries, calendars, work schedules, phone numbers, email addresses, and real property addresses of owners or users of the property listed in **Attachment A**, any potential participants in fraud schemes, potential witnesses or victims, financial institutions, or retail establishments;

2. Any and all personal identity and/or financial information of potential participants in fraud schemes or victims;

3. Any and all photographs or video recordings of owners or users of the property listed in **Attachment A**, any potential participants in fraud schemes, potential witnesses or victims, identifiable physical locations, bank checks, financial account information, or other instrumentalities of the fraud scheme;

4. Any and all records, documents, and materials pertaining to identification, including but not limited to, birth certificates, driver's licenses, photo identification cards, passports, visas, Social Security cards, and any use or application for these items;

5. Any and all records, documents, and materials pertaining to bank checks and any bank accounts or other financial accounts;

6. Any and all information documenting or evidencing the existence of conspiracies to commit fraud or identity theft;

7. Any and all records, receipts, or other documentation of retail purchases;

8. Any and all information disclosing the location, travels, and destinations of potential participants in fraud schemes;

9. Any and all information disclosing the use and operation of any device or equipment used to create counterfeit checks;

10. Any and all information or documents pertaining to materials used to produce counterfeit checks; and

11. Any item clearly identifiable as contraband.

II. Law Enforcement Search Protocol

1. The law enforcement search of electronic devices listed in **Attachment A** shall be conducted pursuant to the following protocol in order to minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search are viewed.

2. With respect to the search of any digitally/electronically stored information provided to law enforcement by forensic analysis, the search procedure by law enforcement may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized;

b. opening or reading portions of files in order to determine whether their contents fall within the items to be seized;

c. scanning storage areas to discover data falling within the list of items to be seized, to possibly recover any such deleted data, and to search for and recover files falling within the list of items to be seized; and/or

d. performing key word searches through all electronic storage areas to determine whether occurrence of language contained in such storage areas exist that are likely to appear in the evidence to be seized.

3. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the above listed crimes or other criminal activity, the further search of that particular directory, file or storage area, shall cease.